2010-09-00

Threat-based Response Patterns for Emergency Services Developing Operational Plans, Policies, Leadership, and Procedures for a Terrorist Environment

Threat-based Response Patterns for Emergency Services: Developing Operational Plans, Policies, Leadership, and Procedures for a Terrorist Environment

Robert T. Mahoney

America is at war. Unlike most of America's past wars, this war is being fought simultaneously in multiple locations overseas and within our borders. Our military continues to function in its traditional role as the front line troops overseas, but the frontline duties at home in this war of terrorism have become the responsibility of those who have not been tasked with that previously: America's emergency services.[1]

Several of our communities have been attacked and/or threatened. Thousands of our citizens and hundreds of our emergency personnel have been injured and murdered in this war at home. Yet, there is little in the experience, organization, structure, training and response patterns of the emergency services that have prepared them for this role as war fighters.

Numerous directives and guidelines have been produced at all levels of government concerning preparation, protection, recovery, etc. from terrorist attack,[2] but how to incorporate that information into the day-to-day operations of the emergency services and their response patterns has been largely left to the discretion of the emergency services themselves. How those operational changes develop and evolve will require an understanding of a series of steps and dynamics that will have to be taken at the individual community and departmental levels in order for those agencies to adopt and adapt to their new war fighting tasks.

In spite of the fact that the terrorist threat to the United States has been realized for many years, and even after the disasters of September 11, 2001, not all emergency service departments have fully absorbed the lessons of that day. Some have not coordinated the work of each of their operational and administrative elements *to create response patterns that specifically address this changed and highly dangerous operational environment*. Unfortunately, at times the work of these different elements can become parochial and self-focused, and they may fail to coordinate their response pattern development efforts to reach a collective, functioning, best outcome that benefits the entire department. This condition may be reflective of, among other possibilities, insufficient organizational structure, ineffective leadership, individual personality differences, or a lack of a common understanding of the purpose and primary objectives of the organization itself. Such parochial difficulties, particularly in the current operational environment created by terrorism, can result in a lack of efficiency, a loss of effectiveness, duplication of effort, unnecessary expenditure of funds and resources, loss of public trust and confidence, increased danger to department personnel, and the loss of life and property.

Correcting this condition can be largely addressed through an awareness and adoption of a professional methodology that conforms a department's organization, planning, leadership, functioning, training, and response pattern into one that has a common understanding of the nature of the threat environment and of the fact that the department is involved with war-fighting.

A Form of War

As previously noted, a department responding to terrorism is involved in a form of warfare. In this current state of conflict, it is referred to as "asymmetrical" warfare, which for the purposes of this article will mean the forces, means, and capabilities of the terrorists are dramatically out of balance with that of their enemies. Given that, the terrorist must try to compensate for this imbalance by selecting targets, using tactics and weapons, etc., that provide them with an impact greatly in excess of their size and resources. Since terrorism is a form of unconventional or "asymmetrical" warfare, it is useful to note certain situations from past wars which can highlight the difference between routine and crisis conditions and thinking as regards to response patterns.

The Civil War battle of Antietam was the bloodiest battle ever fought in America. In one day, 22,719 were killed. At Antietam, there is a small, triple arch, twelve-foot-wide stone bridge over the Antietam creek, now known as Burnside Bridge. Union General Ambrose Burnside, following orders, sent multiple waves of soldiers to attack across the bridge. Although each successive attempt was decimated, he nonetheless kept repeating the tactic he had been trained in, which was the then currently accepted method relied on *routinely* in past battles.[3]

Fifty years later, in World War I, French Field Marshal Joseph Joffre, British General Sir Douglas Haig and other allied commanders, sent attack after attack out of the trenches for months, against the German machine guns, at the Battle of the Somme. A half million soldiers died in that one battle; 60,000 British on the first day alone.[4] Joffre, Haig and the other commanders apparently found it impossible to change methods and tactics, or to realize and adapt to the changed threat (weapon) environment.

Both these warfare examples are indicative of a thought process that displays the difference between routine and crisis preparation, thinking, recognition, and response. Both examples demonstrate the use of the *routine* form of thinking and response.

Conversely, the British admiralty had a number of wooden warships under construction on the day they received word of the battle between the first ironclads – the Monitor and the Merrimac – during the American Civil War. They quickly accelerated plans to have iron plates bolted to the sides of their new ships, recognizing that the operational environment had permanently changed and that wooden hulled ships were no longer sufficient and could not serve as the core of their navy.[5] While some senior naval officers probably failed to accept that their routine methods had to be changed, the organization as a whole grasped and understood the *crisis* condition that existed, and started to develop methods that addressed their new operating environment.

The purpose of this article is to consider how a number of operational and administrative skills and abilities, familiar to emergency services but not necessarily suited to meeting the current terrorist condition, should be re-examined and corrected. This article will demonstrate how those familiar elements are not isolated, independent issues, but are in fact parts of a continuum of the same problem (the threat) that must be addressed comprehensively to meet the requirements of, and to operate in, this new terrorist war-fighting environment.

In order to create appropriate response patterns it is first necessary to completely understand the nature of the terrorist threat and risk that a department can be facing,

both generally and to the responding entities specifically. This is done through a risk assessment process.

This article reviews what an emergency service department should understand about the elements of 1) threat, 2) risk, 3) security, 4) resources, 5) crisis leadership, 6) training, and 7) planning. This article then reveals how gaining an understanding of each of these elements both informs and improves all the other elements. Such knowledge enables these elements to be mutually supportive in the development of counter terrorism response patterns. This process uses a series of understandings, transitioning in sequence from one element to the next, and each builds on the previously gained knowledge. These transitions are:

Transition 1: Understanding Threat Informs Risk Analysis

Transition 2: Risk Analysis Informs Security Mitigations

Transition 3: Security Ensures Resource Allocation for Terrorist Events

Transition 4: Terrorist Events Require Crisis Leadership Skills

Transition 5: These Issues, Addressed Through Training and Plans

THE TERRORIST ENVIRONMENT

Records of the Global Terrorism Database at the University of Maryland show that worldwide there have been over 10,000 terrorist attacks on police facilities and officers since 1970.[6] Hospitals have also been attacked as part of wider terrorist actions. In the Mumbai, India, terrorist attack in November 2008, the terrorists attacked the counter-terrorism forces while they were responding from their headquarters, killing several of them, including the commanding chief of the Anti-Terrorist Squad.[7]

The *9/11 Commission Report* noted that Khalid Sheikh Mohammed who planned the attack on the World Trade Center admitted to having sent Dhiren Barot (aka. Issa al Britani) to New York six months before the 9/11 attack to conduct surveillances of the World Trade Center and other targets.[8] The video tapes he made were found in a computer seized in Pakistan in 2005. Barot was sentenced to 136 years in prison for terrorism in the United Kingdom in 2007 and copies of the tapes he made were released to the public by Scotland Yard. Among the targets he photographed and concentrated on were a Fire Department of the City of New York (FDNY) firehouse and the police presence in the vicinity of the World Trade Center.[9]

In the United States, as in other countries around the world, the use of "secondary devices" or bombs, to kill and injure first responders as they arrive at a scene, has been a tactic used by terrorists and is an attack method that first responders and their departments have become aware of. Under such conditions, responding units know they need to have a heightened sense of security as they approach such a scene, but the above information suggests a further threat.

Barot's video taping of a fire station as part of an array of targets, the bombing of hospitals and police stations as *targets themselves* and/or as part of a wider attack on a primary target, is a clear indication that the terrorists understand the high target value these first responder personnel, units, and locations represent. However, recognizing

the possibility of terrorists targeting and attacking the first responder locations and resources – *as prime objectives themselves* – is generally not part of the operations and response planning of first responder units and departments in this country. Past terrorist actions indicate that such occurrences are foreseeable risks that emergency services should consider including in their planning.[10]

The May 2010 attempted car bombing of New York City's Times Square is an instructive event. The initial call transmitted from the police on scene was for a car fire. The first arriving emergency service was the fire department, which responded according to routine protocol to commence a fire suppression operation based on the information that had been received. Due to their counter terrorism awareness, the FDNY quickly assessed and realized that the situation was potentially a vehicle-borne improvised explosive device (VBIED) and took appropriate action. Had this not been done and had the device exploded, it is probable that the department would have again experienced the highest casualty rate among the emergency services.[11]

It is important to understand that, nationally, most of the response patterns currently in place for routine operations are insufficient to address the types of situations a department will encounter in responding to an ongoing terrorist attack such as the Times Square incident. New plans must be created for these situations. There is a process that can be used to assist department leaders and planners in developing threat-based response patterns, one that uses the transition of knowledge gained in each element to assist in the development of the next one. It starts with a fully inclusive risk assessment.

TRANSITION 1: Understanding Threat Informs Risk Analysis

Determining which threats a department faces does not necessarily mean there is an equal risk associated with each of the threats. To develop appropriate response patterns to terrorist threats, a department must convert knowledge of threats into risk.

A formal process of conducting a risk assessment within a department is the initial step in developing plans, policies, and procedures to address operations within the current terrorist environment. Risk assessments use established protocols and algorithms in their analytical process. These protocols can be complex and/or proprietary in nature, depending on which of several available methodologies is selected. The following is a simplified review of the sequence of steps that a risk assessment may contain. It is not a detailed explanation of each of the elements involved in every step of the process, but rather an overview of the objective of the steps leading to an organized indication of risk. With this knowledge a department or organization can proceed to the development of response operations suitable to address the known and identified threats and risks. Without this knowledge a department will resort to guessing about the actual functional condition of their capabilities and counterterrorism profile.

Risk Assessment

The first step in the elimination of internal parochial planning concerns is conducting a risk assessment, and the first part of that is determining the nature of the threat

scenarios the department is likely to encounter. The process described below focuses on the terrorist environment as the specific threat being addressed, as compared to ordinary or routine response circumstances. While it is recognized that the current interest in an "all hazards" approach to planning has significant utility and appeal, the array of situations an emergency department can find itself involved in may already include many, if not all of the naturally occurring, unintended, and accidental emergencies present in an all hazards approach to planning. Departments whose territory and response activity include blizzards, earthquakes, tornados, or other cyclically occurring emergencies may have become prepared and conditioned to manage such matters through years of response to such emergencies. However, large explosive charges, the use of chemical and radiological weapons, directly attacking department locations and personnel, etc., presents a much different set of circumstances for which departments are not as prepared. Existing natural hazard response plans may or may not need up-dating, but planning for and responding to terrorist activity is different than other emergencies.[12] Addtionally, plans based on terrorist risk assessments can bring benefit to departmental capabilities in responding to an "all hazards" environment.

The Risk Assessment process being discussed in this article consists of seven sequential sub-elements: 1) threat, 2) criticality, 3) vulnerability (likelihood), 4) response and recovery capabilities, 5) impact (consequence), 6) risk, and 7) needs.

1. The *threat* component permits a department to identify the types of terrorist weapons it needs to consider and protect against, as well as the means by which each of those weapons can be used against the department. A specific threat is dependent upon the terrorist's objectives, motivations, and capabilities, as well as the target attractiveness of the department's assets to the terrorists.

2. The *criticality* element permits the department to rate the relative importance of each of its assets in accomplishing the department mandate. Establishing this hierarchy of criticality also suggests which assets require protection from the terrorists' methods of attack.

3. The *vulnerability* component evaluates the amount of security an asset has as compared to the possibility of a successful attack upon it. Noting the specific vulnerabilities per type of attack also suggests potential security enhancements to counter those vulnerabilities.

4. The *response and recovery* element measures the capability of the department to respond to and recover from each of the types of attack upon the department itself. This is not to be confused with response patterns for operations in the terrorist environment generally.

5. The *impact (or consequence)* part of the assessment measures the percentage of loss of the assets' criticality to the department that would occur due to a successful attack. This metric also represents the relationship between the

terrorists' capabilities to achieve their objective and the department's ability to protect against it.

6. The *risk* component demonstrates a hierarchical rating of the assets for each type of attack as a result of the threat, vulnerability, and impact analysis. Each of the department assets is compared to every other identified asset to demonstrate their relative risk.
7. The *needs* component permits a department to review various security and recovery solutions that would serve to reduce the level of risk the department faces from a terrorist event.[13]

Threat

In this country, responding to terrorism is an experience limited to a very few emergency services departments. It should therefore be an area of concern for those departments that have not yet considered it as an issue. The range of terrorist threats to a department is identified by the types of weapons used or sought by terrorists. Emergency responders know them as Weapons of Mass Destruction, or WMD. Included in this category of weapons are: chemical, biological, radiological, and nuclear weapons, and explosives. In addition, an analysis of recent terrorist tactics and methods shows that more conventional types of weapons and tactics, associated with the "small unit type actions" displayed in the Mumbai attack, can also be devastating to emergency services. [14]

The likelihood of a department encountering any or all of these forms of attack is a variable driven by the full range of conditions and circumstances unique to each department and its location. A departmental liaison to, or membership in, a regional Fusion Center or a Joint Terrorism Task Force can serve as the source for current and realistic threat information.[15]

Note that the level of existing threat is entirely outside the control of a department when considering WMD's. The amount of threat from these types of weapons is controlled by, and exists solely within, the terrorist element itself and the actual prevention of WMD use is not normally within the capacity of local first responders. Unless the department is capable of neutralizing the terrorist organization itself, or changing the beliefs, objectives, means, or capabilities that drive their attack motivations, the department will not be able to "prevent" an attack. The terrorist organization always retains the option to change the location of its attack to another, "softer" target in order to satisfy its objectives. Thus, that attack is not "prevented," but only "deterred" onto another location.

Criticality

Every department has a mandate or reason for its existence. That reason may be found in enabling legislation, a charter, or mission statement. The initial process in doing a risk assessment answers the question, "What do we do?" The best answer is one that views the department mandate at a high level. For example, for a fire department the answer "We put out fires." is not as comprehensive or accurate as "We prepare for and respond to emergencies that threaten life and property." Opening the range of

possibilities in this manner facilitates thinking about the development of a list of critical assets.

Few departments have assets and resources that are not necessary to some aspect of the department mandate, but not every resource or asset is critical to the mission. The criticality element of the assessment allows a department to evaluate which of its assets are the most important ones for accomplishing its mission.

All departments function as networks of assets and elements that interact with each other, either operationally or administratively or both. It is the linkage and the frequency of linkage between these elements that can define the networked structure of the department and the criticality of those elements.

The terms used for describing the different types of elements in a network are "nodes", "links", and "hubs". A *node* can be a particular building, a piece or type of equipment, or part of a process, etc. The *links* are the elements and/or parts of a process that serve to connect nodes. This can be a physical, administrative, or operational "pathway" that connects or creates interaction between nodes. A *hub* is a node that multiple other nodes link to. The more links there are from other nodes to a particular hub, the more critical that hub becomes.[16]

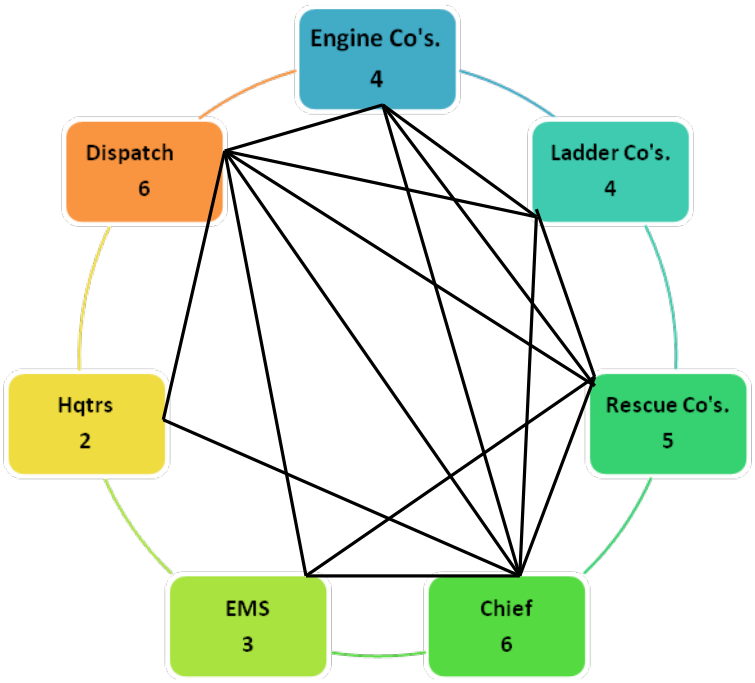

Diagram 1

In theory, the hub with the largest number of links is the most critical in the department network and each of the subsequent hubs have their hierarchy established in a similar manner. While network theory recognizes there are many factors available for use in this calculation,[17] for the purposes of this risk assessment discussion, Diagram 1 displays a notional example of a department's assets on a chart based on the number of

operational communication interactions between some of these elements in a department; many other criteria can also apply.

While each of a department's assets is "critical", it should be clear that each of them is not equally critical. Each critical asset's importance to the range of different factors that make up the department mandate is an indication of its position in a hierarchy of criticality.

These assets, owned and operated by the department, each make an important contribution to achieving the department mandate. Their final position in the hierarchy will reflect an analysis using a common set of factors that make each of them critical to accomplishing the department mandate. Such factors can include the number of casualties that will occur from the loss of this asset, the percentage of the department's ability to function that will be lost due to the loss of this asset, the cost of replacing the asset, etc., but these factors will not apply equally to each asset. Combining the ranked assets with these factors will result in a hierarchy of all the assets' critical relationship to the completion of the department mandate.

Vulnerability

An array of attack weapons and methods are available to the terrorists for them to potentially use successfully against any asset. Clearly, not every weapon would be appropriate for use at each site or against each asset, yet an asset may have a wide spectrum of weapons and tactics that can be used against it.

Note that the use of a particular type of weapon is influenced by many factors external to the department. The objectives of the terrorist element, their chosen means for achieving these objectives, and their capacity for having and using a particular type of weapon are all factors that would be considered. There must be a corollary between the objectives of the terrorist organization, their capabilities and methods, the importance of an asset in achieving (or preventing) their objectives, and the security conditions at the asset to deter the terrorist. Diagram 2 below provides a notional example of how these conditions result in the different types of threat, weapon(s), and attack scenarios that a terrorist might choose to use against an asset, depending upon the particular vulnerabilities of each of the critical assets of the department.

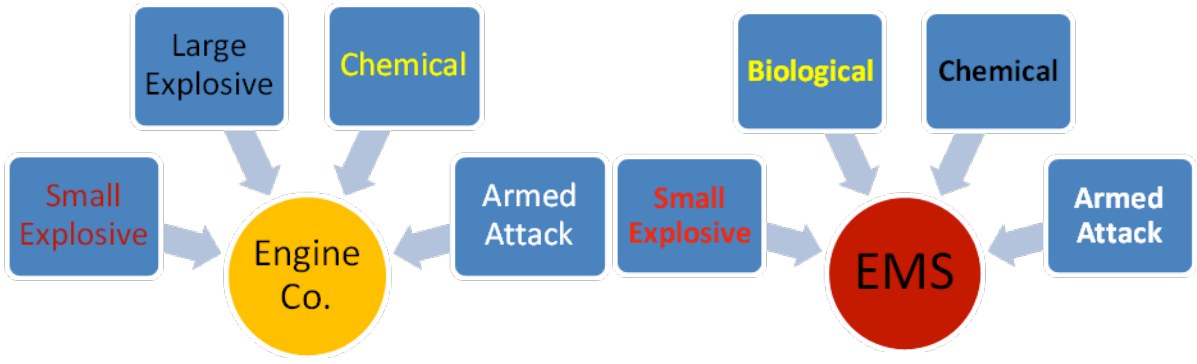

Diagram 2

As revealed above, each of the identified department assets can have a vulnerability to multiple, selected types of attack. Understanding vulnerability consists of knowing both certain specifics about the attack method verses the security conditions that exist at the asset. Some elements of an asset might serve to deter an attack – i.e. the security procedures in place at the asset are believed to be sufficient to deny terrorist access (fences, card readers, etc.) – and such an attack could be detected before it is completed because of other procedures (CCTV, lighting, etc.). There is also the probability that once the attack is detected, it could be interdicted before it is carried out. Other aspects of an asset might be so lacking in security that it would attract an attack. In short, it is necessary for a department to look at itself as the terrorist would in order to determine its vulnerabilities.

It is the difference between the offensive aspects of an attack and the defensive abilities of the asset that provides an indication of the likelihood of a successful attack. If an asset is highly vulnerable to a particular type of attack, and attacking it with a selected type of available weapon would serve the terrorist's objectives, then the probable vulnerability or likelihood of a successful attack at that asset might be high. Conversely, even if the asset is vulnerable but the terrorist element doesn't posses that type of weapon and/or attack capability, or attacking that asset would not serve the terrorist's objectives, then the probability of attack would be lower.

A department can be fully capable of deterring an attack through the introduction and use of security measures that counter specific types of attacks. It is of paramount importance that departments consider security measures to mitigate these types of attack in their planning procedures. It should also be noted that the department's planning must be sensitive to the potential that improperly selected and/or applied security measures may only serve to "deflect" rather than deter an attack. For example, if a department so hardens its administrative building that the terrorists attack a less defended operational building within the same department, then the department has succeeded only in "deflecting" rather than "deterring" attack. In this case it cannot be said that the attack was "prevented".

Response Capabilities

There are specific measures available for preparation for, defense against, and/or response to types of terrorist attack. The department's internal capabilities across a wide range of areas of expertise and resources will be required in the wake of such an attack to continue performing the department mandate. Organizational structure and leadership, the existence of operational plans and procedures, the level of training and expertise, the availability and use of equipment and or systems, and the number and type of personnel and their availability are all primary issues for appropriate response and recovery. The gap between the current readiness condition within the department and a desirable level of readiness in order to continue departmental functionality equates to a department's response needs. For example, if a department needs twenty SWAT trained officers when it currently has eight, or the department has one rescue company but also needs a Haz-Mat capability, such conditions reveal the gap between existing departmental resources and what the current threat environment requires them to have.

Some of the administrative and infrastructure elements of the department also contribute to its response readiness. These includes such things as the presence of administrative plans and procedures, the existence of alternate facilities, communication capabilities, the existence and continuity of vital information in databases, and a periodic use of training exercises. The combination of these operational and administrative elements can reveal the difference between current capabilities and terrorist incident response needs.

Impact

Impact (or consequence) can be described as the portion or fraction of an asset's criticality that would be lost to the department in each of the attack types previously described. This impact is balanced to a degree by determining what fraction of that impact could be reduced or mitigated due to the identified response and recovery capabilities of the department. The combination of these various elements (the percentage of criticality of the assets destroyed, the percentage mitigated by recovery capabilities, and the amount of impact mitigated by response capabilities) has a direct relationship to the overall consequence to the department from these attacks and, by extrapolation, to the surrounding community.

Relative Risk

Relative risk means that assets of different types, with different purposes and functions, being similarly threatened by multiple types of weapons and attacks, can still be measured in direct comparison to each other's level of risk exposure. This also means that all of a department's critical assets can be evaluated as a group.

These risk calculations can be plotted on a graph, where the vertical axis represents vulnerability (likelihood) and the horizontal axis represents consequence (impact), by placing a point on the graph for each type of attack at each critical asset. Those points close to the axis junction (lower left) have less vulnerability and/or consequence than those at a distance from it (upper right). In practice, the assets and attack type combinations proceeding diagonally on the graph up and to the right from the axis point represent the highest level of risk and require the most immediate attention to secure. Since all the assets and attack types are measured against the same set of threats, and each asset has a point on the graph for each type of risk it faces, the plot points display the relative risk between all the assets.

Using this method, it is possible for a department to know that, given its circumstances, the greatest risk may be to their communications center from a vehicle borne explosive, or to their EMS center from a biological weapon, or their headquarters from a chemical attack, or to their rescue company quarters from a man-carried explosive, etc. Each attack type and location will have a position (node) on the graph in direct risk-relationship to every other type of attack at each of the other assets. The below graph displays a notional example of a typical relative risk assessment diagram; an asset can have multiple points on the graph representing each type of attack it could face, while some types of attack appear multiple times against different assets.

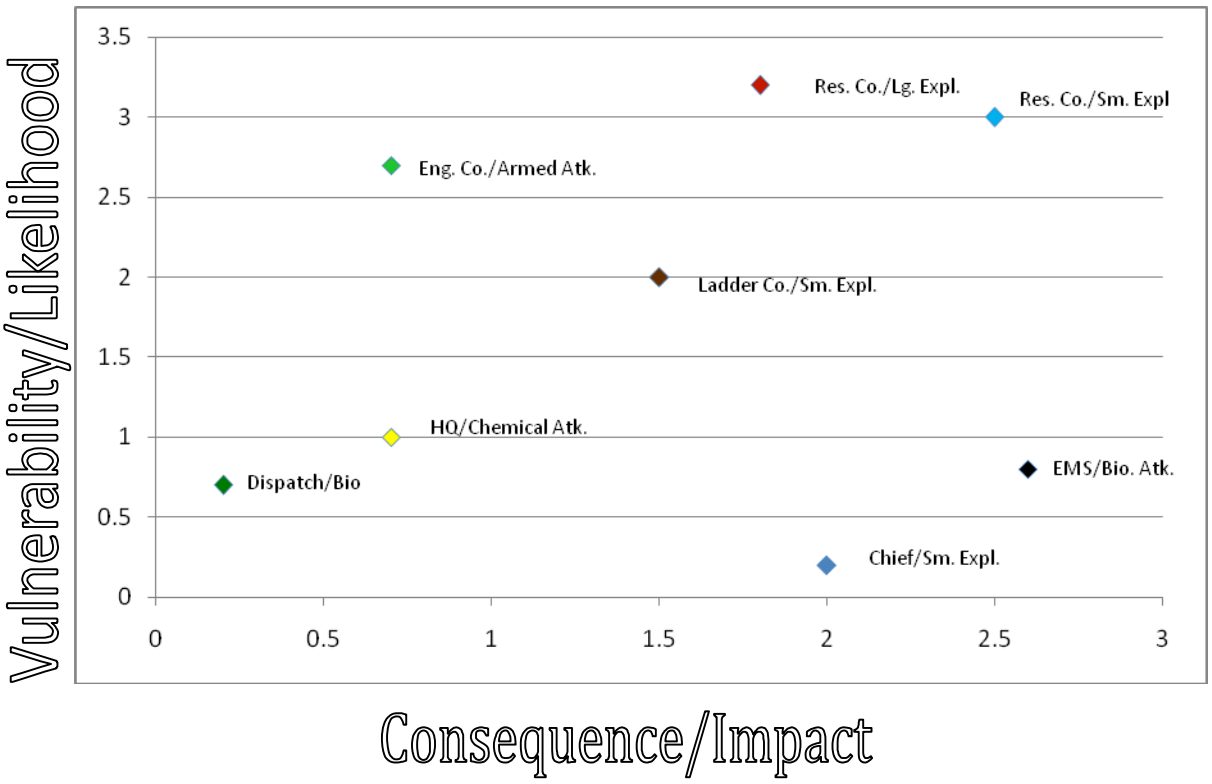

Diagram 3

Needs

Through extrapolation, Diagram 3 also informs department management and personnel of what corrective measures need to be taken in order to lower risk. Determining the reasons for a vulnerability rating suggests the lack of a defensive security measure (or a combination of security measures). Instituting such a security measure (or measures) would serve to lower an asset's vulnerability to a particular type of attack. For example, where a vehicle bomb attack is indicated, the installation of vehicle barriers might serve as a deterrent and installing a type of public access control system could reduce the possibility of a man-carried explosive being used against another asset. Installation of such security measures would lower the risk profile of the involved asset.

Reduction in vulnerability (the vertical axis) is frequently thought of as being achieved through installation of "site-hardening" physical security measures. While this is a logical way to reach the risk reduction goal, other means are also available and must be considered. For example, one of the elements of 'likelihood' is the target's attractiveness to the terrorist; changing that attractiveness is a means of reducing risk. Making a target too difficult to attack, or beyond the terrorist's weapon and resource capability, reduces the target's attractiveness and, therefore, "likelihood". Changes in established operational procedures can also serve to lower risk by making various aspects of the asset less vulnerable.

Risk can also be reduced by making changes in consequence (the horizontal axis). This is frequently done through duplication and/or dispersal of the asset. If destruction

of a particular asset represents a single potential point of failure in accomplishing the department mandate, then consideration can be given to duplicating that capacity and/or dispersing its functional purpose throughout multiple other elements or locations, in order to reduce that failure consequence. Measures that create duplication and dispersal of ability can extend the time during which an emergency service can continue to provide services in a crisis by ensuring a replacement or substitute capacity when a similar function is lost at another location. Note, however, that security measures which reduce consequence without changing the level of vulnerability of assets rely, in part, on the presumption that the terrorist element does not have the capacity to eliminate all of the vulnerable assets simultaneously or each in sequence. Thus, choosing mitigations that focus independently on reducing "likelihood/vulnerability" *or* "consequence/impact" alone can have the desired effect of reducing risk to the asset where they are applied; but a program that develops need-driven mitigations that reduce both these elements of risk (vulnerability and consequence), simultaneously and in coordination with each other, directly enhances overall security and supports the sustainability of the departmental services the asset provides.

Applied risk reduction measures that lower vulnerability can sometimes be dependent on various forms of technology. Departments must be sensitive to the degree of technological dependence created in addressing their risk reduction methods, particularly if the technology represents a single point of failure. If the technology fails or is overcome, the total consequence of the original vulnerability can occur immediately. The level of accrued technological dependency may not permit any time for initiating other measures to limit the full consequence.

In situations where technological dependency is acute, a program that trains personnel not to extend their operations to the extreme limits of the technology and/or provides alternate methods to achieve the objective, can serve to increase actual safety and available time to avoid the full consequences of any technological failure.

Whether the choice to reduce risk applies to vulnerability or consequence, or ideally both, it is important to remember that the mitigations and changes driven by the needs assessment should not be limited to physical and structural changes alone. Operational changes in routine functioning are often highly effective in reducing risk, usually involve less capital costs than physical changes, and can be applied more easily and often on a scale that varies according to the current local level of threat. It is often most effective to implement both physical and operational risk reduction efforts in a coordinated manner. It is in this area that changing response patterns as a result of specific terrorist conditions can be highly effective.

Return on Investment

Investments in counter-terrorism mitigations can be significant and as with all investments, must present a gain or positive return for the investor. The gain being sought in a risk assessment is the reduction of risk. It is that reduction which represents the return on this investment, and each mitigation must have a value in risk reduction with a direct relationship to the recognized threats. The cost of each mitigation method and/or a combination of mitigations, and their effectiveness and efficiency in gaining risk reduction per actual unit of cost, is a major issue for a department. By using pre-

and post-mitigation installation assessments, a department will be able to evaluate its overall security profile at any given time and the return on investment of its mitigations. It should be understood that the assessment profile and all aspects of risk respond to the nature of the threats, which can change over time. It is therefore beneficial for a department to periodically reassess its threat and risk condition.

Additionally, department management must consider the concept of "acceptable risk" in selecting which asset(s) are chosen, and in what sequence for mitigation improvement. Presuming that available funding in any given year will be insufficient to address the totality of mitigation needs, a department must choose how and where those funds will be expended. Logic would seem to dictate that the asset determined to be most at risk (see Diagram 3, Rescue Co./Small Explosive) would be the first asset to receive corrective measures, and each subsequent asset in the hierarchy would be addressed in turn according to available funding. Another method could be to collectively fund partial mitigation for a selected group of assets, or all assets simultaneously, thereby giving some protection to a wider group of assets rather than in-depth security to one. Regardless of which process is chosen, the gap between the optimum obtainable security condition desired, and that which current funding, technology or expertise permits, is the amount of 'acceptable risk' a department will have until conditions allow further mitigations to be applied or the threat itself diminishes.

Similarly, a department must guard against selecting a method of mitigation simply because it has the highest return on investment. Expending funds for that reason only, on an asset that holds a lower position on the risk assessment graph, leaves those higher ranked assets wanting for attention.

TRANSITION 2: Risk Assessment Informs Security Mitigations

Security Mitigations

The vast majority of calls that fire departments and emergency medical services respond to are accidental. That is to say, they are not intentionally caused. The exceptions of arson and other intentional criminal matters account for a select percentage of the total responses, but most departments consider such operational responses within their routine patterns. The idea that these emergency services may themselves be intentionally targeted is rarely considered or planned for. This is not to be confused with any existing plans for operating under dangerous conditions or in a contaminated zone; these plans envision *arriving at* an ongoing, unusual, or terrorist event wherein something else is the primary target. The concept being considered here is that of *emergency services being directly targeted and attacked* as part of a wider terrorist event. Departments have an awareness of time-delayed "secondary" explosive devices being planted for the specific purpose of impacting emergency responders upon arrival, but the intentional attacking of the services *prior to or concurrent with* a wider attack is not an event generally included in emergency planning.

There are numerous examples of terrorist attacks targeting security forces whose expertise could impede or deny the terrorists' attack objectives. Such actions as attacking command and control hubs, communications centers, hospitals, etc. that can

reduce the impact of the terrorist attack by rapid and effective use of a department's responding capabilities are such examples.[18] By neutralizing or minimizing that response capability the asymmetry of the attack shifts in favor of the terrorists.

Both captured intelligence evidence and past terrorist actions require that this intentional targeting potential be examined.[19] Causing death, injury, and destruction are some of the primary intentions of transnational terrorists. Terrorists have demonstrated that they can improve their effectiveness in those areas through the elimination or lowering of the response capabilities of local authorities.[20] Recent evolutions of such attacks, particularly in Mumbai, India, have clearly demonstrated that the terrorists were able to enhance the effects of their attacks through such means. Whether conducting pre-attack surveillance on emergency services, rehearsing attacks on responding vehicles, attacking police stations, commandeering emergency vehicles, or executing response commanders, there is ample evidence to indicate that such tactics are part of their overall planning.[21]

Emergency services must realize that they represent some of the most valuable and finite counter-terrorism resources in the country. This means that departments should highlight the need to secure their resources from attack and take the possibility of any diminished capability or capacity due to such situations into account in their policy development and response planning and budgeting.

Even if departmental resources are not targeted directly, multiple types of WMD terrorist attacks are capable of wide-spread injury, death, and destruction. Emergency services are not immune from such consequences. These types of attacks can seriously impact both on-duty and off-duty personnel, and equipment serviceability, simultaneously. Crisis planning considerations should examine the departmental response profile through a range of diminishing levels of personnel and equipment availability due to the direct impact of a particular type of attack on the resources of the department itself, or by its being effected by these WMD. There is a direct relationship between the number, and capabilities, of the remaining department resources following an attack, and the selection of which emergency operational functions are to be continued at which critical community locations. There is a "tipping-point" at which operations are unavoidably or intentionally diminished.[22] This point will vary from department to department. Note that a departmental capability should never be confused with its capacity. A department may have excellent training, equipment, leadership, and experience to address an event – even a terrorist event – but its ability to rapidly respond and sustain those operations over time or in simultaneous multiple attack scenarios is a measure of its capacity,[23] which can be dramatically reduced by WMD.

The above risk assessment process can identify which assets are most at risk from terrorist-type attacks and their current vulnerability profiles. In planning terrorist response operations, senior emergency management needs to consider actions and expenditures that will help ensure that their most valuable resources (frequently the ones most at risk) remain viable and available for use by the wider community during and after these emergencies.[24] Even a cursory review by senior management will often reveal that the entirety of a department's policies, practices, and particularly Standard Operating Procedures (SOP), have been created to function in a routine environment

and will therefore need to be completely reconsidered to ensure survivability in a terrorist attack. Physical site hardening of critical assets and the installation of access-limiting measures that create a secure zone in depth, as well as operational changes, are some of the basic steps that can be taken to help protect these resources. Such hardening is not limited to physical sites; it should include mobile resources as necessary. In every instance it is the selection of the correct mitigation or (more frequently) a combination of mitigations, chosen because they are directly mapped to a risk reduction need identified through the above risk assessment process, that will be the most effective in addressing security concerns.

TRANSITION 3: Security Ensures Resource Allocation for Terrorist Events

The above risk assessment process results in a department understanding the ways in which it is threatened by terrorism and which of its assets are most vulnerable to that threat. The process also identifies those assets that will need to be secured from those threats since they are the most necessary and critical for the department to carry out its mandate in the event of a terrorist attack. That understanding of all aspects of risk is necessary in order to examine and address a department's preparedness profile for responding to terrorism. One of the principle ways of determining preparedness is to understand the way a department allocates resources.

Resource Allocation

"What is our capacity to do what we do"?

For an emergency services department, the answer to this question is related to all the resources that attach to each of the department's critical assets, and all other assets, in order to accomplish the department mission. For example, a fire department may have twenty apparatus including pumpers, ladder trucks, ambulances, rescue vehicles, mobile command vehicles, etc. The number of them and the total number of personnel assigned to those operational functions, in addition to those in administrative functions, can give an indication of the department's response capacity. That distribution will reflect what local experience and practice has shown to be the appropriate number of resources necessary to meet the daily routine requirements of the department. Diagram 4 (below) demonstrates the possible assets and the number of emergency personnel distributed within a department.

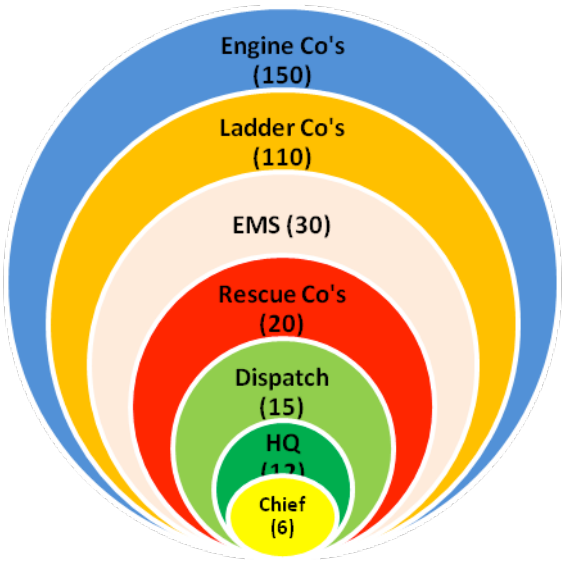

Diagram 4

"How do we accomplish our mission?"

The answers to this question generally involve training, command and control, response patterns, communication systems and data bases, liaison and mutual aid, etc. Knowing the answers to these questions permits a department to have an overarching view of its functional means and processes necessary to operate. Specifically, it will have an analysis of its daily, routine operations and how the department mandate is met.

"What resources, and in what numbers, will be needed to respond to each type of terrorist event?"

Diagram 5 (below) hypothetically lists an asset, the number of personnel assigned to that type of asset, and the types of WMD that asset will be called on to mitigate. (Diagram 5 is not intended to be comprehensive.)

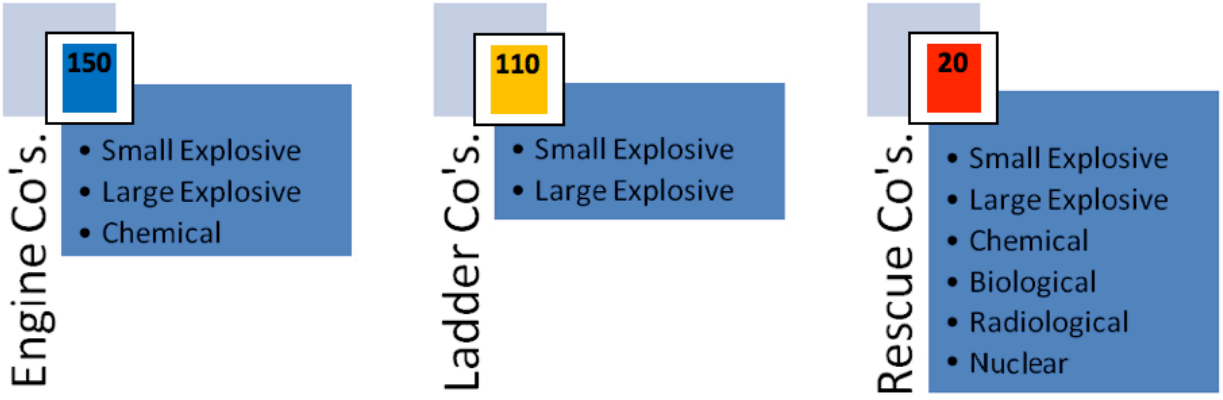

Diagram 5

Risk assessments (particularly in the response capabilities section) provide an analysis of critical issues and critical needs when operating in a *WMD* environment. The distribution of resources shown in Diagram 4 describes resource allocation for *routine* operations and functions.

As displayed in Diagram 5, the WMD response resource allocation needs are clear. The two diagrams (4 and 5) are dramatically different. In fact, the distribution of routine function resources (for example, personnel) may be nearly inversely proportional to the department needs in addressing the WMD terrorist threat. In Diagram 5, note that there are 150 personnel assigned to engine companies who can operate in response to three types of WMD attack, but only twenty rescue personnel available for addressing six types of WMD attack. Multiple, simultaneous attacks of this type would only serve to exacerbate this issue.

The reason for this disparity is that response to a routine matter and response to a terrorist/crisis event are two entirely different circumstances, requiring very different operational processes, abilities, and resources.

The expertise, equipment, and resources used most infrequently in daily operations will become some of the very elements in greatest demand during response to a terrorist event. Attempting to use the larger routine resources as a substitute for them during a crisis can/will result in great peril to those resources and an inadequate outcome for the conditions being addressed. This situation would be a crisis for the department.

TRANSITION 4: Terrorist Events Require Crisis Leadership Skills

The above description of a department's resources provides an indication of how it is prepared to respond to the full range of its mandated duties. But, as can be seen, those duties do not always consider the potential for terrorism within a department's response protocols. Similarly, the on-scene command and control of those resources may also not calculate the leadership issues – particularly the relationship between resource allocation, response patterns, and leadership present at a terrorism event.

Routine versus Crisis Response

Due to an emergency department's experience, training methods, management practice, and organizational structure and culture, the ability to recognize a crisis and to respond accordingly with methods specifically designed for a crisis (if such methods even exist) often develops too late in the course of the crisis to mitigate the issue. Unfortunately, for some the recognition does not come at all.

A crisis is often viewed is as a calculation of the size or scale of the event, but this is not always justified. For example, transmitting a fifth alarm for a fire, or calling up the police reserve, clearly signifies the occasion of a large-scale event. But this is not necessarily a crisis, inasmuch as the department has these existing methodologies and resources available to address the problem. In short, the department has a means in place to address large, but routine, matters. Conversely, a single police officer, suddenly engaged in a shootout with multiple armed subjects, is very much in a crisis status. Thus, size or scale alone is not always a legitimate measure for determining the presence of a crisis; there is a difference between routine – meaning something prepared for and

regularly addressed regardless of size – and a crisis, which is neither routine nor prepared for and can either evolve or be sudden and unanticipated.[25]

This ability to recognize the difference between routine and crisis conditions is a pivotal issue for emergency service leaders in a terrorist war environment.

Crisis Leadership

In studies of failure to manage crises, including those involving homeland security-type issues, Harvard's Kennedy School of Government has examined the crucial elements in decision making during situations that move from "ordinary" or routine, to "high consequence" or crisis conditions.[26] The point at which the routine (Status R), moves to crisis (Status C) is largely dependent on the amount of "novelty" in the situation and how quickly those in charge are able to recognize, and respond to, the novelty or newness of the situation. Status R is identifiable by its "familiar" elements and Status C by its "unfamiliar" ones. Individuals, institutions, and societies succeed or fail based on which set of elements is permitted to dominate the response in times of novelty or crisis.

Routine vs. Crisis Elements

Status R contains the following elements: a need for minor customizing; has standard operating procedures and clear objectives; has sufficient resources, policies, and laws; has sufficient training; has clear authority and organizational structure; is expert driven; has some unknowns; and plans are based on known threats.

Status C contains the following elements: it invalidates some standard responses; there is a mismatch between the problem and resources, policies, laws, and experience; it requires capability based planning; and it has "unknown unknowns."

Routine vs. Crisis Leadership

Status R leadership elements display: a familiarity with the condition; a substantive expertise with the issue; a consultative/directive style of leadership; demonstrated interpersonal skills ability; and a reliance on recognition-primed ("I've seen this before") decision making.

Status C leadership elements display: an expertise in multiple operations; a flexible "first responder" mindset; a strong personality; risk taking ability; a willingness to create a wide organization (a "sudden network"); rapid assessment of network abilities (evaluates resources); focuses the network (identifies what is important); decisiveness (takes command).

Recognizing Routine vs. Crisis Situations

A true crisis is characterized as an event which: has high stakes and high costs; is beyond existing resources; consumes available resources; has serious negative outcomes; entails a realization that a standard response is inadequate; and requires action that is urgent and imperative. There is a loss of control, the size and complexity of the situation is expanding, there is command and/or operational confusion, there is a lack of authority to act or too many authorities involved, it has high political and media attention, it is a unique occurrence or scale, it is beyond what has been prepared for, and there is a high level of uncertainty.

A "novelty" or crisis can also be characterized as a situation that changes from *categorized* to decentralized, *bureaucratic* to improvisational, *big picture control* to a possibility of risk, and from *familiar reliance* to a need for trust.

As the situation moves from Status R to Status C, the challenge is to not let the "R" people and/or methods maintain control according to routine practices, because the situation can no longer be overcome by using familiar methods. The main objective in overcoming a crisis is to apply creativity, improvisation, and rapid innovation – or prepared response patterns whose elements have that built-in crisis capacity as compared to routine responses.

The most common and systemic mistakes made by otherwise bright people in addressing crisis constitute cognitive failures which are most likely to occur under pressure. These mistakes are created by: over valuing one's own experience; believing in an illusion of experience (discounting what we haven't seen ourselves); and multiple forms of overconfidence, such as believing there is an understanding of the entire situation, all the facts are known, being able to make predictions, having a capacity to influence outcomes, and being able to control events.

Actions based on those types of cognitive failure are characterized by: continuing a commitment to an irrational action through escalation of that commitment; bounded awareness or focusing on the wrong things; over reliance on readily-available data; overconfidence; searching for data that confirms pre-conceived beliefs (a valid information bias); and an action orientation that has a preference to avoid risk (which in crisis only increases risk).

Routine vs. Crisis Indicators

Routine *(STATUS R)*	Crisis *(STATUS C)*
The situation is familiar	**The situation is a unique occurrence or scale**
Uses standard operating procedures	**Is beyond what has been prepared for**
Has clear objectives	**There is a high level of uncertainty**
There are sufficient resources	**The problem is beyond the existing resources and/or all resources are consumed**
The resources are the correct ones	**Resources do not match the problem**
The outcomes are expected and normal	**Has serious negative outcomes**
Authority and organizational structure is clear	**There is a lack of authority to act or too many authorities overlapping**
Is expert driven	**Experience is not equal to the task**
Plans are based on known threats	**Requires capability based planning**
Has some unknown conditions	**Has unknown unknowns**
Response needs minor customizing	**Invalidates some standard responses**
The threat level is normal	**There are "high-stakes" involved**
The cost is acceptable	**The cost is high**
Action time is normal	**Action is urgent and imperative**
Command is direct and obeyed	**There is command and/or operational confusion and a loss of control**
It attracts no or normal attention	**Has high political and media attention**
It can be contained with normal responses	**Has expanding size and complexity**

Diagram 6

What the generals were facing in the earlier warfare examples was a Status C situation which they were addressing with Status R process. Their actions represented a "cognitive failure" (as evidenced among other of the above indicators) by the fact that they were "continuing a commitment to an irrational action through escalation of that commitment." Reviewing the accounts of both battles and the nature of the wars in which they occurred, the descriptions of "crisis" and the failures to recognize the "novelty" of the situation that existed in the Harvard criteria are plainly evident, along with the failure of leadership to respond in an effective way partly due to their inability to recognize crisis.

Clearly, the British admiralty example is the opposite circumstance.

Routine vs. Crisis Leadership Skills

Routine (Status R)	*Crisis (Status C)*
Familiarity with the condition	**A flexible mind-set**
Has substantive expertise with the issue	**Expert in multiple types of operations and can rapidly assess network capabilities (evaluates resources)**
Has strong interpersonal skills and consultation/direction style	**Has a strong individual "take command" personality**
Reliance on "recognition primed" decisions	**Quickly recognizes the "novelty" of the situation. Is a risk taker and can focus the network (identifies what is important) and a willingness to create a wide organization (a "sudden network")**

Diagram 7

The principle hazard for emergency services in terrorist events (or other forms of crisis), in addition to the direct hazard of being targeted themselves by terrorists, is the failure to recognize the crisis condition for what it is, as rapidly as possible. Any command delay in switching from 'routine' to 'crisis' operations status can result in disastrous outcomes. Yet the very nature of emergency service response patterns and culture can aggravate this problem; i.e. departments do not traditionally have separate, prepared, and practiced "crisis" response protocols that the commander and operational personnel can switch to when the situation requires it.

Emergency services have well-established methods for managing large or expanding emergencies. This is most frequently done through sounding additional alarms, calling in mutual aid, applying the Incident Command System (ICS), etc.,[27] which is a universally accepted and practiced process. But a WMD crisis is not just another large emergency; it is a "novel" situation that must be immediately recognized and managed according to plans and response procedures designed specifically for these events. In fact, a routine plan (such as Mutual Aid or ICS) that facilitates an ever-expanding response and use of additional resources, might create the illusion of control and can serve to delay the critical command recognition that a crisis is occurring which requires a different type of response.[28] It is of primary concern that all departments develop such crisis awareness and terrorist/crisis-specific operational plans. This will serve to make

them more effective in a crisis in their own jurisdictions or when responding under mutual aid or ICS.

The discussion thus far has examined the nature of the threat, the consequences of an attack, and the need for changed response patterns to address those threats. However, the information developed also indicates that a department can do more than just "respond". It can also take measures to protect itself from being victimized by the terrorist attacks.

TRANSITION 5: These Issues are Addressed through Training and Plans

As can be seen from the above, for an emergency service operating in a terrorist environment, the relationship between threat, resources, leadership, and response patterns is an all important equation. The balance between these elements can be critical to the department successfully achieving its mandated objectives. That balance is gained by making the necessary changes to each of these elements in relation to the others, and it is within the department planning and training programs that the most significant and effective changes can occur and must begin.

Training Systems

Emergency services train their personnel to operate within a practiced and coordinated system and process designed to be highly effective and efficient. Significant amounts of time and money are allocated to ensuring that every member of the department is fully aware of his or her duty, and has the knowledge and means to execute those duties properly. The nature of emergency work is such that repetitive conditioning through training and exercises ensures that each member will respond to a situation in a manner that has been tested and shown to be effective in gaining the desired outcome. The training is often conditioned to the point of individual operators responding instinctively. This methodology is designed to create teamwork and organization that focuses all resources on achieving the desired outcome in the most effective and efficient manner. This orchestrated response pattern is nearly universal and contains within its normal parameters the capability to meet and address expanding emergencies. In short, training methods condition personnel to address situations that have known best practices available, regardless of the scale of the event.

These training programs are experiential at their core. Many years of analysis of what happened, what worked, and what proved to be the best solution has evolved into Standard Operating Procedures (SOP). It is absolutely mandatory that such methods be developed and applied in daily operations because they represent the collected knowledge of years of experience that result in the most effective and efficient means of responding to an event. These events that training addresses vary by location, frequency and scale, but the thing that remains constant is that, regardless of these dynamics, all are familiar events. The very fact that training protocols exist for these conditions is *prima facie* evidence that the condition is a known occurrence for which best practices have been derived through experience. The vast majority of all emergency services rely on the effective use of these inculcated response patterns by their personnel to carry out

the mandate of the department. Such training is at the core of effective emergency management practices for *routine* events.

Unfortunately, the SOP can also lead to response patterns in individuals and organizations that become more automatic and habitual rather than considered. It is this reliance on routine actions that can be a primary issue in growing a crisis into a disaster. Reliance on known event parameters, and a matching response pattern by a department and every individual in it, reflects the core strength of the organization and can also become its greatest weakness.

The longer the delay in recognizing that a crisis is occurring, and then changing response patterns accordingly, the worse the outcome can be.[29] It must also be understood that even if a leader recognizes the existence of a crisis, but has only routine resources and response processes available to use, that leader will be overmatched and forced to rely heavily on improvisation, which will meet with limited success and duration.

Therefore, the pivotal factors in addressing crisis are *situational awareness* (having knowledge of the totality of an event), the amount of *time* that has elapsed before crisis recognition is made, and having specific *crisis response plans available*. All these issues can be managed by training programs.[30]

Training Sources

Just as SOP are created by experience, the fact that only a select few domestic emergency services have first-hand terrorist operations experience precludes the ability of others to develop new response patterns from their own knowledge. Those departments that do have such experience most likely dealt with a singular event, which is certainly not sufficient to draw upon for response plan development for the full range of terrorist-type attacks. Limited experience can tend to isolate and focus departmental thinking to anticipate a repetition of what has happened to them previously, causing them to develop too narrow a plan.[31] It is therefore mandatory that terrorist-based response patterns be developed by accessing the wealth of information that has been gained as a result of decades of worldwide responses to these events.

While the attempted New York Times Square car bombing, in May 2010, initially appeared routine, several issues created a note of caution for responding units: Times Square is clearly a high value, iconic target location; the vehicle was hastily left in a marked pedestrian cross-walk rather than in a parking space; there were unusual "popping noises" coming from the vehicle; there was white smoke without heat; and the vehicle was immediately abandoned by the driver.[32] None of these factors individually might be sufficient to trigger a heightened awareness on the part of the responding units, but in the aggregate, where crisis training protocols are comprehensive, they serve to give warning that a possible terrorist event is underway. It is understood that initial responding units rarely have full information about the conditions they will encounter and can therefore be drawn into an environment they would otherwise avoid. That lack of information is one of the cautionary indicators of crisis that enhanced training can include.

As previously noted, one of the keys to successful crisis management is the ability on the part of the personnel involved to recognize that the environment they find

themselves in is in fact, a crisis.[33] It may seem odd to suggest that experienced individuals might not recognize the novelty of their situation, or that it is actually a crisis, but the historic military examples given previously are only representative of numerous such examples across the full range of human experience, including the emergency services. Inasmuch as modern terrorist objectives bring a form of warfare into the realm of the emergency services, it is imperative that those services be prepared to address and counter these events with training and preparations at a level, and on a scale, that have previously been thought of as matters confined to war and military leaders and decision makers.

Training Curriculum

Training for Crisis Leadership

Any crisis can also contain "routine" elements that will be familiar to an experienced leader. The presence of such elements can cause a cognitive failure, where the leader focuses on the wrong things (a bounded awareness) and develops a myopic view of the entire situation. The leader is in danger of making overly focused decisions that rely on "recognition primed" thinking, when in fact the entirety of the environment calls for decisions that cannot be judged by experience alone.[34]

Operational leadership training programs that rely on stress-inducing scenarios to test a commander's ability to acquire, distribute, and utilize ever-expanding resources, serve to accustom that individual to managing a wide range of disparate facts and details simultaneously.[35] It is essentially a test of the individual's ability to manage the growing minutiae of an incident. Such repetitive attention to the management of details can occur at the expense of overall situational awareness and unacceptably extend the time it takes to recognize that a crisis condition exists.

Inducing stress can be an effective teaching method, but it must be counter-balanced with a process that teaches the leader to regularly detach from issues of detail in order to rethink and re-evaluate the totality of the operation in order to recognize crisis situations sooner and to take appropriate action.

Alternatively, resources permitting, a secondary leader can be assigned the duty of continuously monitoring and evaluating the entirety of the situation rather than its minutiae, and serve as an assistant/advisor to the commander. Such a position would provide the commander with a second source of warnings, cautions, and critical advice in determining the existence, and managing, of the crisis.[36]

Providing Crisis Response Tools

At the heart of the matter is the fact that due to the lack of specific crisis response status training, let alone counter-terrorist training, even if emergency personnel do recognize that they are in a crisis, they are left with no other methodologies for response available to them other than those designed to address routine conditions.

Clearly, because of the culture of these organizations, their personnel are highly innovative and will quickly regroup and reorganize in a way that eventually develops a successful, if limited, path for them to follow. However, in the face of an enemy that has factored emergency service methods and capabilities into its attack plans, the terrorist overmatching of the department response capabilities may cause that innovative

response pattern to be ineffective or to come long after the terrorist's objectives have been met. In short, departmental innovations may come at a time when they can be applied to the "recovery" phase, rather than during the crisis management part of the event. Thus it is manifest that the amount of time expended to first become aware of the crisis situation, and second to apply alternative procedures to counter the crisis, are two critical issues in regaining control of the operating environment.

It is insufficient to train personnel to recognize the presence of a crisis, but not have crisis protocols and/or response patterns for them to utilize during the crisis. As noted above, such a situation will leave the leaders and other personnel relying on innovation and improvisation alone to address the situation. While emergency service personnel are often innovative by nature, the ability to innovate (which is different from improvisation) is a highly personal and singular matter. Given similar circumstances, or even separate parts of the same incident, an innovative response that is dependent on the variables of personal ability and preference can result in drastically different outcomes for the same conditions. In the absence of crisis protocols, opportunities for innovative and/or improvisational response will soon be overmatched by the growing crisis condition. Additionally, recognizing that improvisation requires spontaneous and rapid reorganization and instruction, significant modification of protocols, and the use of tools, equipment, and technology for purposes for which they were not intended, means small chance for success of continued and repetitive improvisation during a crisis.

Routine Training and Crisis Training

A training program that establishes an additional crisis response training course parallel to the routine matters course can start to address the modern form of terrorist warfare in its operational area. In essence it means providing instruction in two different forms of thinking and operating, based on threat recognition. Traditionally, emergency services do not teach multiple, alternative forms of operations and the departments' themselves are not organized, managed, or equipped to function along parallel tracks. This, however, is the very functional condition that effectively combating transnational terrorism has imposed upon emergency services.

The first step in establishing a crisis training regimen is to instruct all personnel to recognize the signs that differentiate crisis (Status C) from routine (Status R). It is then necessary to have a command and operations structure that is authorized and capable of immediately changing the department from routine to crisis operations and administration as soon as the crisis is recognized. Most importantly, it is necessary for the training and command entities to have established crisis policies, plans, procedures, and resources in place that can be substituted during crisis for the now inadequate routine methods.

This is not to say that routine procedures become discarded or obsolete; it is within the scope of the department mandate that an emergency service will continue to respond to other routine matters concurrent with the crisis occurring. However, the crisis use of available resources will severely impact the scale and ability of the department to respond to the routine matters, requiring significant modification to existing routine response patterns as well.[37] It is this requirement to maintain both forms of response in parallel that will have a significant impact on policy changes. The

intensity and level of threat will determine if a department uses dual, parallel response patterns for routine and crisis matters simultaneously, or chooses to use crisis response mode for all activities to counter the potential consequences of sudden terrorist events leading to injury and loss of department personnel in such an environment.

RESPONSE PLANNING

The modification of all of the elements of an emergency services department discussed thus far is driven by understanding the nature of the threat and the relationship of each of the departmental elements to the other. Changing all of those relationships in a balanced and cohesive manner, utilizing the sequence of transitions described above, will require a department to develop detailed plans based on the consideration of thoughts and issues about terrorism that may not currently be included in the overall management vision. Department leaders must consider a wide range of new and changed issues.

Planning Considerations

Simultaneously considering altered and/or random, non-traditional response patterns, set to specific types of events, can enhance the potential security of a department's and a community's valuable resources. A response pattern structured to meet current, factual conditions rather than future, presumptive environments, can result in both successful and acceptable outcomes within the dynamic created by these terrorist environments.

Similarly, a review of policies based on administrative and legal matters may reveal the need for additional authority or relief from certain other requirements, in order to fully function in this changed environment. Virtually every area of a department's functioning – from contracting to recruiting, equipment purchasing, supply management, communicating, housing, and promotions, etc. – can be modified to update and enhance a department's security and operational capabilities profile both during, and in the aftermath of, one of these incidents.

As the threat of terrorist activity increases, through various notification means we have come to recognize (such as the yellow to orange, orange to red, etc.) a department can order different types of operations. For example, "Secure Response Conditions" under "orange" conditions can mean changing response routes, responding only with police escort,[38] blocking private vehicles from transiting roads used by critical departmental assets, etc.

A further heightened threat level may result in a "Limited Service Response Condition" wherein departmental resources are retained away from critically hazardous or ongoing situations until such time as the immediate danger passes. This response can also serve to ensure the survival of those resources for use in protecting the wider community.[39]

Such overarching departmental policy and training alterations do not come easily. The realization that every aspect of a department culture will undergo some change is a significant concept to grasp and adjust to. It is also probable that those very individuals on whom this change-management task will fall are the same individuals who have the longest association with the reliability of the established routines. Conversely, they are also the individuals who have the greatest knowledge of the department and all its

networked aspects. They should therefore be the most capable of identifying and coordinating all the cause-and-effect relationships that a modification of one element will require in all the other elements.

The sequence of the risk assessment, threat-based resource allocation process, crisis leadership issue, and training needs alluded to earlier can serve as the pivotal guide in managing these terrorism-motivated departmental changes. As a department enters into this process it is worth noting the following items:

- A conceptual model for dual routine and crisis thinking and management can be found in the military practice of designating a "General Quarters" condition. All routine matters cease, all personnel change immediately from a routine to a crisis mind-set, and all operations, equipment, resources, and response patterns become crisis condition-based for the duration of the situation.
- Ensuring the security of critical assets before an incident will positively contribute to the availability and sustainability of those resources during and after a terrorist event and crisis.
- Planning for crisis by starting with current departmental conditions and resources and working to evolve into a crisis-ready format may not be efficient. Consider deciding on the desired departmental outcome or 'end-game' for operating in a terrorist-induced condition, and work backwards to determine what training, procedures, and equipment need to be developed in order to ensure the department's desired outcome. Also calculating potential departmental losses created by the terrorist event will help determine the priority and scope of subsequent operations and departmental capabilities.[40]
- Do not project personal or departmental standards of behavior onto the terrorists' planning and practices. Instead, rely on the stated objectives of the terrorists themselves to anticipate the issues that need to be addressed. Rather than trying to predict specifics, use the change in preparedness and the improved ability of the department to meet and counter the terrorist objectives as the measurement of reorganizational success.[41]
- It is of primary importance that each department member not only knows his or her individual responsibility in the crisis procedure, but also what is the intended purpose and outcome of the operations plan in total. This is done so that every member can continue to work to achieve that outcome despite any mishaps or plan failures caused by the terrorists. This allows leadership initiative to surface during crisis.
- Do not plan to counter what the terrorists *are going to do* – this is a presumption based on knowledge of their past actions. Absent any specific knowledge of actual plans, departmental thinking and planning from this basis seriously limits the potential to create operations and security measures that can be highly effective against terrorist attacks. In essence, this is "planning for the last war" and is an example of a hindsight bias. Instead, plan for what the terrorists *are capable of doing*, which is based both on their past actions and current capabilities, using knowledge provided by the department's intelligence agency partners. Such

thinking will keep the department current with the latest threat, and ensure that mitigations and plans serve to match or overmatch the terrorist abilities, thereby reducing departmental assets' target attractiveness.

CONCLUSIONS

Traditional emergency services are operating in the front lines of combating and responding to terrorism. The response protocols used by these departments are based on routine emergencies and are insufficient to meet the direct threat of terrorist incidents. In order to understand and meet the current level of threat, these departments must re-examine conditions, security, and response capabilities through a series of steps beginning with a comprehensive risk assessment. Emergency services departments must ensure the security of their personnel and critical assets, re-define the allocation of resources, prepare for crisis leadership, and develop training methods and response patterns that reflect the nature of the current threat environment. These elements must be viewed as a continuum of inter-related parts of the same problem, rather than individual, independent issues. Creating threat-based response patterns will challenge all the assumptions on which current routine-based response patterns exist.

Command personnel charged with developing these protocols must resist the temptation to fall back on what has been done previously under routine response conditions. In fact, many of the protocols developed to respond to a terrorist threat will seem to be the antithesis of the very culture of the department itself and may be met with significant resistance both internally and externally. All the parties involved must understand, be trained, and be prepared to operate in both routine- and crisis-status situations that are different, because a terrorist crisis condition *is* different from the daily, routine condition. The current reality of the terrorist threat and departmental risk exposure requires that a prepared emergency services department make these changes.

By starting with an understanding of the current terrorist threat, and using the knowledge gained in each step of the above processes to inform the successive steps, a department will overcome the parochial approach to developing its response patterns. A department can become informed and transformed to counter the terrorist threat, protect its personnel, fulfill its mandate, and continue to serve the community it protects in this new terrorist environment.

Robert T. Mahoney is a retired FBI agent who served as the national manager for all FBI Special Operations Groups, assistant legal attaché for terrorism in London, and acting assistant special agent in charge in New York. He was in the World Trade Center on September 11th and a supervisor in the FBI Crisis Command and Recovery Center thereafter. After retiring from the FBI, Mahoney was a team leader in the development of the WMD Terrorism Threat and Vulnerability Assessment process for Critical Infrastructures, and general manager of security programs for the Port Authority of New York. He holds a master's degree in education and another from the Naval Postgraduate School in national security studies. Mr. Mahoney may be reached at r.mahoney@manageemergencies.com.

[1] United States Congress, *Homeland Security Act of 2002*, Public Law 107, 107th Cong. (November 25, 2002), 6 USC.101, Sect. 2, http://fl1.findlaw.com/news.findlaw.com/wp/docs/terrorism/hsa202.pdf

[2] The White House, *Homeland Security Presidential Directive 8, National Preparedness* (Washington, DC: U.S. Department of Homeland Security), 1 (2.d), http://www.dhs.gov/xabout/laws/gs_1215444247124.shtm#1

[3] S. W. Sears, *Landscape Turned Red* (New York: Houghton Mifflin Company, 1983).

[4] S.L. A. Marshall, ed., *The American Heritage History of World War I* (New York: American Heritage Publishing Company, Inc., 1964).

[5] R.K. Massie, *Dreadnought* (New York: Random House, 1992).

[6] National Consortium for the Study of Terrorism and Responses to Terrorism, *Global Terrorism Database* (University of Maryland, College Park, 2009-2010)2010, july 8), www.start.umd.edu/gtd/search/results.aspx?page=1&casualties_max=&target=3&charttype=live&chart=overtime&ob+GTDID&od=desc&expanded+yes#results-table

[7] A. Rabasa et al., *The Lessons of Mumbai* (Santa Monica, CA: RAND Corporation, 2009).

[8] The National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York: W. W. Norton & Company, 2004), 150.

[9] R. Windrem, "Al-Qaida's NYC Surveillance Video Release," *MSNBC,* June 15, 2007, http://www.msnbc.msn.com/id/19254592/ns/nightly_news/print/1/displaymode/1098

[10] Rabasa et al, *Lessons of Mumbai;* S. Gale, L.A. Husick, and L. Rabinow, *E-Notes Messages from Mumbai: Terrorism and Policy Implications* (Foreign Policy Research Institute, January 2009), 1-2, http://www.fpri.org/enotes/200901.galehusickrabinow.mumbai.html.

[11] Fire Department, City of New York. (2010). *Textbook Response at Times Square Car Bomb Incident,* Supplement No. 23 to *Department Order No. 35*, 2.1.1 (New York: New York City Fire Department, 2010).

[12] Ibid., 10.

[13] U. S. Department of Homeland Security, *Risk Management for Special Needs Jurisdictions* (Washington, DC: Office of State and Local Government, Coordination and Preparedness, Office for Domestic Preparedness, n.d.)

[14] U. S. Department of Homeland Security, *Attack on Pakistan Police Academy Highlights New Terrorist Emphasis on Small-Arms Tactics* (Washington, DC: Office of Intelligence and Analysis, 2009).

[15] Bureau of Justice Assistance, *Fusion Center Guidelines-Developing and Sharing Information in a New Era* (Washington, DC: U. S. Department of Justice, Office of Justice Programs, 2006).

[16] T.G. Lewis, *Critical Infrastructure Protection in Homeland Security* (Hoboken, NJ: John Wiley & Sons, 2006).

[17] Kimberly I. Shoaf, Hope A. Seligson, Samuel J. Stratton, and Steven J. Rottman, *Hazard Risk Assessment Instrument* 1st ed. (Los Angeles, CA: UCLA Center for Public Health and Disasters, January 2006).

[18] National Consortium, *Global Terrorism Database*.

[19] Windrem, "Al-Qaida's NYC Surveillance Video."

[20] U. S. Department of Homeland Security, *Ambush-Style Tactics Used Effectively Against Sri Lankan Cricket Team in Pakistan* (Washington, DC: Office of Intelligence and Analysis, 2009).

[21] Rabasa et al., *Lessons of Mumbai,* 21, 22.

[22] B.A. Jackson, K.S. Faith, and H.H. Willis, *Evaluating the Reliability of Emergency Response Systems for Large-Scale Incident Operations* (Santa Monica, CA: RAND Corporation, Homeland Security and Defense Center, 2010).

[23] Fire Department, City of New York, *Terrorism and Disaster Preparedness Strategy* (Brooklyn, NY: Fire Department, City of New York, 2007).

[24] McKinsey & Company, *McKinsey Report – Increasing the FDNY's Preparedness* (New York: FDNY, 2002).

[25] N.N. Taleb, "Learning to Expect the Unexpected," *New York Times*, April 8, 2004.

[26] Author's notes from Leadership in Crises course at Kennedy School of Government, Harvard University, April 2007.

[27] G.A. Bigley and K.H. Roberts, "The Incident Command System: High Reliability Organizing for Complex and Volatile Task Environments," *Academy of Management Journal* 6 (December 2001): 1281-1299.

[28] District Fire Chief M. McNamee, interview with author, July 23, 2008, Worchester, MA.

[29] Ibid.

[30] R. T. Mahoney, "Deciding Who Lives: Considered Risk Casualty Decisions in Homeland Security" (master's thesis, Naval Postgraduate School, Center for Homeland Defense and Security, December 2008), 186.

[31] Gale, Husick, and Rabinow, *E-Notes Messages from Mumbai.*

[32] Author's notes from FDNY Battallion Chief's Command Course, Fire Department of New York, June 2010.

[33] Deputy Fire Chief V. Dunn (ret.), interview with author, June 26, 2008, 20.

[34] Author's notes, Leadership in Crises.

[35] FDNY "Battallion Chief's Command Course".

[36] Ibid.

[37] McKinsey & Company, *Increasing the FDNY's Preparedness.*

[38] Rabasa et al., *Lessons of Mumbai,* 11.

[39] McKinsey & Company, *Increasing the FDNY's Preparedness.*

[40] Jackson, Faith, and Willis, *Evaluating the Reliability of Emergency Response Systems.*

[41] N.N. Taleb, N. N., *The Black Swan* (New York: Random House, 2007).